Załącznik nr 3 do procedury bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej w okresie epidemii COVID-19

**KARTA OCENY SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH (PIA)**

1. **Informacja o Administratorze Danych**
2. Administrator danych:

Nazwa Administratora: Szkoła Podstawowa nr 21 im. Ks. Stanisława Konarskiego w Częstochowie

Adres: **ul. Sabinowska 7/9, 42-202 Częstochowa**

NIP: 573-02-12-013; REGON: 000712462

Tel. 34 3658597

e-mail: sp21@edukacja.czestochowa.pl

1. Inspektor Ochrony Danych: Justyna Sprycha
2. **Informacje o procesie oceny**
	1. Numer karty oceny: 01
	2. Podstawa wykonania oceny: art. 35 ust.1 RODO
	3. Data oceny: 12.05.2020
	4. Wersja oceny: 1.1
	5. Ocenę skutków (PIA) wykonał: Renata Krystek
	6. PIA monitorował: Justyna Sprycha
3. **Kontekst oceny**
	1. **Czynność przetwarzania**: praca zdalna poza siedzibą administratora danych
	2. **Osoby/komórki odpowiedzialne**: dyrektor placówki
	3. **Własność procesu:** czynność własna
	4. **Zakres danych osobowych w czynności**: utrwalenie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesyłanie, udostępnianie, usuwanie lub niszczenie danych osobowych za pomocą programów/platform wykorzystywanych do pracy zdalnej i przetwarzanych informacji
	o uczniach, ich rodzicach oraz pracownikach, między innymi imię, nazwisko, data
	i miejsce urodzenia, dane teleadresowe, PESEL, informacje dotyczące sytuacji zdrowotnej/prawnej/rodzinnej, dane dotyczące przekonania religijnego, informacje
	o rozwoju psychofizycznym i postępach edukacyjnych ucznia, frekwencji na zajęciach, wizerunek oraz inne dane osobowe wymagane przepisami prawa, czasie pracy
	w systemach informatycznych i odwiedzanych stornach internetowych.
	5. **Krótki opis funkcjonalny**: praca realizowana jest poprzez:
4. platformy/ programy (w tym poczta elektroniczna), w których placówka oświatowa
jest administratorem danych, w tym przypadku zawarta jest umowa powierzenia przetwarzania danych osobowych z dostawcą usług;
5. prywatne platformy/ programy (w tym poczta elektroniczna) wykorzystywane do pracy zdalnej – jednostka systemu oświaty nie ma wpływu na zakres udostępnionych danych osobowych i nie odpowiada za poziom zabezpieczeń. Administratorem danych
są właściciele platform/ programów. Pracownik akceptuje we własnym zakresie polityki prywatności i regulaminy platform/programów.
6. dokumentacja papierowa – pracownicy, którzy otrzymali polecenie pracy zdalnej mają możliwość wyniesienia, korzystania i opracowywania dokumentacji papierowej niezbędnej do realizacji obowiązków służbowych.
7. **Wymagania dotyczące czynności przetwarzania**
	1. **Cel przetwarzania danych**: realizacja obowiązków służbowych w ramach pracy zdalnej
	2. **Podstawa prawna**:
8. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2019 r. poz. 1148 z późn. zm.)
9. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1974 Nr 24 poz. 141 z późn. zm.)
10. Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych
z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 374 z późn. zm.)
11. Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku
z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. 2020 poz. 410
z późn. zm.)
12. Rozporządzenie Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczegółowych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. 2020 poz. 493 z późn. zm.)
13. Art. 6 ust. 1 lit e RODO - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
	1. **Adekwatność zbieranych danych w stosunku do celu**
14. W przypadku platform/programów, w których placówka oświatowa jest administratorem danych: zbierane dane są adekwatne do celu.
15. W przypadku prywatnych platform/ programów: brak wpływu na zakres udostępnionych danych osobowych.
16. W przypadku dokumentacji papierowej: zbierane dane są adekwatne do celu.
	1. **Prawidłowość zbieranych danych**
17. Pracownicy przetwarzają dane osobowe zawarte w dokumentacji papierowej
i elektronicznej poza siedzibą Administratora danych na podstawie polecenia pracy zdalnej.
18. Pracownicy posiadają upoważnienie do przetwarzania danych osobowych adekwatne
do zajmowanego stanowiska pracy.
19. Dane osobowe aktualizowane są automatycznie, w sposób ciągły przy użyciu systemu informatycznego.
20. Używanie nowych platform/programów przez pracowników wymaga zgody Administratora danych.
21. Dane osobowe przetwarzane w formie papierowej są ograniczone.
	1. **Okres retencji danych**

Dane osobowe przechowywane są zgodnie z przepisami prawa:

1. Jednolitym Rzeczowym Wykazem Akt;
2. platformy/programy wykorzystany do pracy zdalnej, na czas pracy zdalnej (rozporządzenie MEN).
	1. Z**asady powierzenia danych**:
3. w przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych zawierana jest umowa powierzenia przetwarzania danych osobowych;
4. w przypadku platform/programów, w których jednostka systemu oświaty nie jest administratorem danych: pracownik samodzielnie akceptuje politykę prywatności
i regulamin.
	1. **Przetwarzania danych poza UE**

Dane osobowe przekazywane są poza UE.

* 1. **Opis spełnienia obowiązku informacyjnego**

Klauzula informacyjna dla pracowników do umowy o pracę (akta osobowe). Ponadto
w poleceniu pracy zdalnej zawarte są podstawy prawne przetwarzania danych w czasie epidemii COVID- 19.

* 1. **Opis zbierania zgody**

Zgoda nie jest pobierana.

* 1. **Opis sposobu realizacji praw**
1. W przypadku platform/programów, w których jednostka systemu oświaty jest administratorem danych osoby oraz dokumentacji papierowej – osoby, których dane dotyczą mogą dochodzić swoich praw poprzez wystąpienie z wnioskiem do administratora danych.
W procesie przetwarzania posiadają następujące prawa:
* prawo do bycia poinformowanym – realizowane,
* prawo dostępu do danych – realizowane na żądanie,
* prawo sprostowania - realizowane na żądanie,
* prawo do usunięcia - realizowane na żądanie,
* prawo do sprzeciwu - realizowane na żądanie,
* prawo do ograniczenia - realizowane na żądanie.
1. W przypadku platform/programów (w tym prywatna poczta elektroniczna pracownika),
w których jednostka systemu oświaty nie jest administratorem danych nie ma możliwości realizacji praw osób, których dane dotyczą.
2. **Identyfikacja zagrożeń o wysokim poziomie ryzyka naruszenia**

Tabela 1. Zagrożenia o wysokim poziomie ryzyka naruszenia praw lub wolności osób, których dane dotyczą

|  |  |  |
| --- | --- | --- |
| **IDENTYFIKACJA AKTYWÓW** | **RYZYKO I SZACOWANIE** |  |
| **Grupa aktywa** | **Waga aktywa** | **Aktywo** | **Właściciel aktywa (ryzyka)** |  |  |
| *Zagrożenie* | ***Poziom Ryzyka*** |
| Ludzie  | **4** | Pracownicy administratora  | **Administrator danych** | błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem | Ryzyko wysokie |
| **4** | niewykorzystywanie/ brak służbowej poczty elektronicznej do pracy zdalnej | Ryzyko wysokie |
| **4** | brak/nieznajomość procedur pracy zdalnej | Ryzyko wysokie |
| **4** | nieuprawniony dostęp do danych osobowych | Ryzyko wysokie |
| **4** | używanie tych samych haseł/ zapamiętywanie ich w różnych systemach informatycznych  | Ryzyko wysokie |
| **4** | brak szkolenia z zakresu pracy zdalnej | Ryzyko wysokie |
| **4** | niewylogowanie się z programów/ systemów informatycznych | Ryzyko wysokie |
| **4** | nieprawidłowe zabezpieczenie sprzętu przed kradzieżą, uszkodzeniem lub zniszczeniem | Ryzyko wysokie |
| **4** | niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych | Ryzyko wysokie |
| Oprogramowanie | **3** | Programy/ platformy wykorzystywane do pracy zdalnej | przypadkowa lub niezgodna z prawem utrata danych osobowych | Ryzyko wysokie |
| Urządzenia  | **4** | Prywatny sprzęt: laptop, komputer, telefon, tablet, itp. | brak zabezpieczeń urządzenia/plików zawierających dane osobowe | Ryzyko wysokie |
| **4** | współdzielenie sprzętu z wieloma osobami | Ryzyko wysokie |
| **4** | ujawnienie danych osobom nieupoważnionym (min. poprzez wgląd) | Ryzyko wysokie |
| **4** | korzystanie z nielicencjonowanego oprogramowania, brak aktualizacji | Ryzyko wysokie |
| **4** | wykorzystywanie sprzętu nie tylko do celów służbowych | Ryzyko wysokie |
| **4** | nieprzestrzeganie / brak znajomości zasad korzystania z prywatnego sprzętu w celach służbowych ustalanych z pracodawcą | Ryzyko wysokie |
| Informacje  | **3** | Dokumentacja papierowa | brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. pozostawienie dokumentów w niezabezpieczonej lokalizacji, umożliwienie wglądu osobom trzecim | Ryzyko wysokie |
| **3** | brak ewidencji wydanych pracownikom dokumentów zawierających dane osobowe | Ryzyko wysokie |
| **3** | niewłaściwe brakowanie dokumentacji, np. wyrzucenie do kosza, nie użycie niszczarki do dokumentów | Ryzyko wysokie |
| **3** | Dokumentacja elektroniczna | brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. brak haseł dostępu do plików/dysków/komputera | Ryzyko wysokie |
| **3** | niewłaściwe brakowanie dokumentacji |  |
| Wykonawcy | **3** | Platformy/programy do pracy zdalnej | brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych | Ryzyko wysokie |

1. **Wpływ na osoby, których dane dotyczą**
	1. **Identyfikacja ryzyka**

Główne zagrożenia dla osób zgodnie z zagrożeniami wskazanymi w tabeli nr 1.:

1. utrata poufności,
2. utrata integralności,
3. dostępność danych.
4. **Opis skutków**
	1. **Główne skutki dla osób, których dane dotyczą przy materializacji ryzyka**:
5. kradzież lub fałszowanie tożsamości,
6. utrata reputacji,
7. cyberprzemoc,
8. straty materialne,
9. zwiększenie niepożądanej korespondencji e-mail,
10. utrata kontroli nad danymi,
11. ograniczenie możliwości realizacji praw,
12. dyskryminacja.
	1. **Ocena niezbędności i proporcji**

Charakter przetwarzanych danych osobowych, kary finansowej oraz straty wizerunkowe grożące Administratorowi z tytułu utraty poufności, integralności i dostępności informacji powodują, że stosowane zabezpieczenia ochrony danych osobowych nie są wystarczające. Dlatego wymagane jest wprowadzenie działań minimalizujących ryzyko naruszenia praw
i wolności osób, których dane dotyczą.

1. **Ocena skutków**
	1. **Stosowane zabezpieczenia minimalizujące ryzyko:**
2. środki techniczne i organizacyjne zgodne z polityką bezpieczeństwa ochrony danych osobowych i instrukcją zarządzania systemami informatycznymi,
3. umowy powierzenia przetwarzania danych osobowych.
4. **Planowane działania**
	1. **Planowane do wdrożenia zabezpieczenia minimalizujące ryzyko:**
5. wprowadzenie procedury przetwarzania danych osobowych podczas pracy zdalnej;
6. ograniczenie przetwarzania danych osobowych w przypadku platform/programów,
w których jednostka systemu oświaty nie jest administratorem danych;
7. szkolenia dla pracowników z zasad bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej.
8. **Ocena Zagrożeń**

Tabela 2. Ocena zagrożeń

|  |  |
| --- | --- |
| **IDENTYFIKACJA AKTYWÓW** | **RYZYKO I SZACOWANIE** |
| **Grupa aktywa** | **Aktywo** |  |  |  |  |  |
| *Zagrożenie* | *Prawdopod.* | *Skutek* | ***Ryzyko*** | ***Poziom Ryzyka*** |
| Ludzie  | Pracownicy administratora  | błędy ludzkie spowodowane np. nieuwagą lub zmęczeniem | 3 | 1 | **12** | Ryzyko wysokie |
| niewykorzystywanie/ brak służbowej poczty elektronicznej do pracy zdalnej | 3 | 1 | **12** | Ryzyko wysokie |
| brak/nieznajomość procedur pracy zdalnej | 4 | 1 | **16** | Ryzyko wysokie |
| nieuprawniony dostęp do danych osobowych | 3 | 1 | **12** | Ryzyko wysokie |
| używanie tych samych haseł/ zapamiętywanie ich w różnych systemach informatycznych  | 3 | 1 | **12** | Ryzyko wysokie |
| brak szkolenia z zakresu pracy zdalnej | 4 | 1 | **16** | Ryzyko wysokie |
| niewylogowanie się z programów/ systemów informatycznych | 3 | 1 | **12** | Ryzyko wysokie |
| nieprawidłowe zabezpieczenie sprzętu przed kradzieżą, uszkodzeniem lub zniszczeniem | 3 | 1 | **12** | Ryzyko wysokie |
| niezgłoszenie administratorowi danych naruszenia ochrony danych osobowych | 3 | 1 | **12** | Ryzyko wysokie |
| Oprogramowanie | Programy/ platformy wykorzystywane do pracy zdalnej | przypadkowa lub niezgodna z prawem utrata danych osobowych | 4 | 1 | **12** | Ryzyko wysokie |
| Urządzenia | Prywatny sprzęt: laptop, komputer, telefon, tablet, itp. | brak zabezpieczeń urządzenia/plików zawierających dane osobowe | 4 | 1 | **16** | Ryzyko wysokie |
| współdzielenie sprzętu z wieloma osobami | 4 | 1 | **16** | Ryzyko wysokie |
| ujawnienie danych osobom nieupoważnionym (min. poprzez wgląd) | 3 | 1 | **12** | Ryzyko wysokie |
| korzystanie z nielicencjonowanego oprogramowania, brak aktualizacji | 3 | 1 | **12** | Ryzyko wysokie |
| wykorzystywanie sprzętu nie tylko do celów służbowych | 4 | 1 | **16** | Ryzyko wysokie |
| nieprzestrzeganie / brak znajomości zasad korzystania z prywatnego sprzętu w celach służbowych ustalnych z pracodawcą | 3 | 1 | **12** | Ryzyko wysokie |
| Informacje | Dokumentacja papierowa | brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. pozostawienie dokumentów w niezabezpieczonej lokalizacji, umożliwienie wglądu osobom trzecim | 4 | 1 | **12** | Ryzyko wysokie |
| brak ewidencji wydanych pracownikom dokumentów zawierających dane osobowe | 4 | 1 | **12** | Ryzyko wysokie |
| niewłaściwe brakowanie dokumentacji, np. wyrzucenie do kosza, nie użycie niszczarki do dokumentów | 4 | 1 | **12** | Ryzyko wysokie |
| Dokumentacja elektroniczna | brak zabezpieczeń danych osobowych w miejscu wykonywania pracy zdalnej, np. brak haseł dostępu do plików/dysków/komputera | 4 | 1 | **12** | Ryzyko wysokie |
| niewłaściwe brakowanie dokumentacji | 4 | 1 | **12** | Ryzyko wysokie |
| Wykonawcy | Platformy/programy do pracy zdalnej | brak umów powierzenia z wykonawcami gwarantujących prawidłowe przetwarzanie danych | 4 | 1 | **12** | Ryzyko wysokie |

1. **Ocena działań**

Ze względu na sytuację epidemiologiczną jednostka systemu oświaty nie miała możliwości przygotowania niezbędnej infrastruktury i dokumentacji w zakresie bezpiecznego przetwarzania danych osobowych zawartej w dokumentacji papierowej oraz elektronicznej podczas pracy zdalnej. Szczególnie nowe przepisy dotyczące realizacji zajęć szkolnych
w formie pracy zdalnej dają szeroką możliwość realizowania przez nauczycieli zajęć
z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu kształcenia,
w tym z wykorzystaniem środków komunikacji elektronicznej. Pozostawiają zatem jednostkom systemu oświaty dużą swobodę odnośnie wyboru właściwego narzędzia przy uwzględnieniu wszystkich aspektów związanych z możliwościami placówki, nauczycieli, a przede wszystkim, biorąc pod uwagę możliwości techniczne i organizacyjne rodziców i uczniów. Dlatego
do pracy zdalnej nie są wykorzystywane wyłącznie służbowe programy/platformy (w tym prywatna poczta e-mail) i sprzęty, np. laptopy. Wobec powyższego w opinii Administratora danych zachodzi wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą,
w szczególności w przypadku:

* programów/platform, w których jednostka systemu oświaty nie jest administratorem danych (prywatne adresy e-mail, komunikatory typu Messenger lub WhatsApp );
* prywatnego sprzętu pracownika, na przykład laptopa;
* przetwarzania danych osobowych w lokalizacji zewnętrznej, którym jest mieszkanie pracownika.

W związku z powyższym nie ma kontroli nad danymi osobowymi w dokumentacji dotyczącej uczniów, rodziców i pracowników jednostki systemu oświaty.

Dlatego też, na dzień analizy zostały zaplanowane działania zaradcze przedstawione w pkt. 9.

……………………….... …………………………………………………………

 *Data podpis i pieczęć Administratora Danych*